REMARKS/ARGUMENTS

1. Claims 1, 2, 8-14, 16, 17, 21-28, and 34-40 are Patentable Over the Cited Art

The Examiner rejected claims 2, 8-14, 16, 17, 21-28, and 34-40 as anticipated (35 U.S.C. §102) by the newly cited Davis (U.S. Patent No. 5,473,692). Applicants traverse.

Independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: maintaining keys of computer systems authorized to access software to be distributed; receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined key if there is one determined key; determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the generated message transmitted to the second computer system; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

The Examiner cited col. 7, lines 30-64, col. 8, lines 33-65 and col. 9, lines 15-22 of Davis as disclosing the requirements of these claims. (Seventh Office Action, pgs. 2-3). Applicants submit that for the following reasons the cited art does not disclose the claim requirements of determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined key if there is one determined key.

The cited col. 7 discusses how a public/private key pair may be generated and sent to a certificate system to make sure that the generated public key is unique. The cited col. 8 discusses how a first hardware agent is authenticated with a second hardware agent. The second

hardware agent transmits a challenge message to the first hardware agent. The first hardware agent decrypts the challenge message with its private key and generates a response encrypting the decrypted challenge message with the public key of the second hardware agent. The second hardware agent decrypts the response wit its private key and compares the original challenge message to the decrytped response from the first hardware agent. (Davis, col. 8, lines 45-60).

Nowhere does the cited Davis anywhere disclose that the authenticating node, e.g., the cited second hardware agent corresponding to the claimed first computer system, determine whether there is one key for the second computer system (corresponding to the cited first hardware agent) that can be used to decrypt the message and then decrypting the encrypted response from the claimed second computer system. In the cited Davis, the cited second hardware agent does not need to determine whether there is one maintained key for the first hardware agent to use to decrypt the message having the challenge response because the message was encrypted with the public key of the second hardware agent, not a key specific to the first hardware agent. Thus, in the cited Davis, the second hardware agent uses its own private key to decrypt the response having the challenge response, not a key for the first hardware agent that is maintained.

In other words, nowhere does the cited Davis anywhere disclose the claim requirement of determining a key for the second computer system to use to decrypt the message. Instead, the cited Davis has the second hardware agent, corresponding to the first computer system, use its own private key to decrypt the response having the challenge message, not a key maintained for first hardware agent, corresponding to the second computer system.

The claims further require that the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. The cited Davis does not disclose this requirement because the cited second hardware agent (corresponding to the claimed first computer system) does not use the presence of a key maintained for the first hardware agent to authenticate the first hardware agent. In fact, the presence of a key for the first hardware agent is not at issue in the cited Davis for this claim requirement, because the second hardware agent uses its own private key to decrypt the message, not a key maintained for the first hardware agent as claimed. Further, according to the cited col. 8, the second hardware agent authenticates the message based

on the presence of the proper challenge response, not the availability of a key maintained for the first hardware agent.

The cited col. 9 mentions that the first hardware agent initates a request for the license token to operate the software if the second hardware agent has a valid license token. Nowhere does this cited col. 9 disclose the above discussed requirements for determining whether the second computer system is authorized to access the software based on the presence of one maintained key for the second computer system (corresponding to the first hardware agent) requesting access.

Further, the cited art does not disclose that a first computer system maintains keys of computer systems authorized to access the software, where the keys are used to determine whether a computer system is authorized to access the software. Instead, the above discussed Davis discusses how the second hardware agent, authenticating the first, uses its own private key to decrypt the message, not a key maintained for the first hardware agent requesting access or authentication.

For all the above reasons, the amended claims 1, 16, and 27 are patentable over the cited art, because the cited Davis does not disclose all the claim requirements.

Independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system and require that the second computer system perform: providing a key to the first computer system capable of decrypting an encrypted response from the from the second computer system; transmitting a request for the software to the first computer system; receiving an encrypted message from the first computer system; processing the encrypted message to generate a response message; encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system; transmitting the encrypted response message to the first computer system; and receiving access to the requested software in response to the encrypted response message.

The Examiner cited the above discussed sections of Davis in rejecting independent claims 12 and 25. (Seventh Office Action, pgs. 4-5) Applicants traverse for the following reasons.

Nowhere does the cited Davis disclose that the a second computer system (requesting access to the software) encrypts a response message to the first computer system, wherein the

first computer may use a key provided by the second computer system to decrypt the response message to receive access to requested software in response to the encrypted response message.

The cited col. 8 of Davis mentions that the first hardware agent (requesting authorization) encrypts a response comprising the decrypted challenge message with the public key of the second hardware agent. (Col. 8, lines 50-60) Nowhere does the cited Davis disclose that the first hardware agent (corresponding to the claimed second computer system) encrypts the challenge message that can be decrypted with a key the first hardware agent provides to the second hardware agent (corresponding to the claimed first computer system). Instead, in the cited Davis, the first hardware agent encrypts the message with the public key of the second hardware agent.

For all the above reasons, claims 12 and 25 are patentable over the cited combination, because the cited Davis does not disclose all the claim requirements.

Claims 2, 8-11, 13, 14, 17, 21-24, 26, 28, and 34-40 are patentable over the cited art because they depend from one of claims 1, 12, 16, 25, and 27, Moreover, the following discussed dependent claims provide additional grounds of patentability over the cited art for the following reasons.

Claims 9, 22, and 35 depend from claims 8, 21, and 34 and further require that encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise public keys from the authorized computer systems, wherein processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

The Examiner cited the above discussed sections of Davis as disclosing the additional requirements of these claims. (Seventh Office Action, pgs. 5-6) Applicants traverse.

The claims require that the first computer system maintain public keys from authorized computer systems and use the requesting second computer system's public key to decrypt the response with the maintained public key. The cited col. 8 of Davis mentions that the second

hardware agent (corresponding to the claimed first computer system) decrypts the message from the first hardware agent (corresponding to the claimed second computer system) including the challenge response with its own private key. The cited Davis does not disclose that the second hardware agent decrypts the message including the challenge response with a public key from the second computer system. Further, nowhere does the cited Davis disclose that the second hardware agent maintain public keys from multiple authorized first hardware agents to use to decrypt their challenge response.

Accordingly, claims 9, 22, and 35 provide additional grounds of patentability over the cited art.

Claims 10, 23, and 36 depend from claims 1, 16, and 27 and further require that the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

The Examiner cited col. 8, lines 33-35 of Davis as disclosing the limitation of configuration data of these claims. (Seventh Office Action, pg. 6) Applicants traverse.

The cited col. 8 mentions that the first hardware agent, requesting authentication, outputs a message including its unique authentication device certificate to the second hardware agent. Nowhere does this cited col. 8 anywhere disclose that the message sent by the second hardware agent (corresponding to the claimed first computer system) include a request for configuration data from the first hardware agent (corresponding to the claimed second computer system). Further, nowhere does the cited col. 8 disclose that the second computer system precesses the response to determine whether the configuration data is for a system authorized to access the computer software. Instead, the cited col. 8 mentions a unique device certificate, not a request and consideration of configuration data of the requesting system (first hardware agent) as claimed.

Accordingly, claims 10, 23, and 36 provide additional grounds of patentability over the cited art.

Claims 11, 24, and 37 include requirements found in claims 9, 22, and 35, such as that the encrypted response is encrypted with a private key of the second computer system and that the

maintained keys comprise public keys from authorized computer systems. Accordingly, claims 11, 24, and 37 provide additional grounds of patentability over the cited art for the reasons discussed with respect to claims 9, 22, and 35.

Claims 14, 26, and 39 include requirements found in claims 9, 22, and 35, such as that the second computer system encrypts the response with its private key, and that the public key made available by the second computer system to the first computer system is used to decrypt the response from the second computer system. Accordingly, claims 11, 24, and 37 provide additional grounds of patentability over the cited art for the reasons discussed with respect to claims 9, 22, and 35.

2. Claims 3, 18, and 29 are Patentable Over the Cited Art

The Examiner rejected claims 3, 18, and 29 as obvious (35 U.S.C. §103(a)) over Davis. Applicants traverse and submit that these claims are patentable over the cited art because they depend from one of claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above.

3. Claims 4, 15, 19, and 30 are Patentable Over the Cited Art

The Examiner rejected claims 4, 15, 19, and 30 as obvious (35 U.S.C. §103(a)) over Davis in view of Scheier. Applicants traverse and submit that these claims are patentable over the cited art because they depend from one of claims 1, 12, 16, and 27, which are patentable over the cited art for the reasons discussed above.

4. Claims 5, 6, 31, and 32 are Patentable Over the Cited Art

The Examiner rejected claims 5, 6, 31, and 32 as obvious (35 U.S.C. §103(a)) over Davis in view of (U.S. Patent No. 5,994,307). (Seventh Office Action, pg. 10) Applicants traverse this rejection on the grounds that these claims depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited col. 7, lines 22-30 and col.

6, lines 40-67 of Komura as teaching the time stamp claim requirement. (Seventh Office Action, pg. 10) Applicants traverse.

The cited cols. 6 and 7 of Komura discusses how a a time stamp is attached to a packet and how the time stamp is used. However, Komura concerns the use of a time stamp with a packet for communicating the packet. (Komura, col. 1, lines 5-12). Nowhere does the cited Komura teach or suggest the use of a time stamp as a random component used to determine whether a second computer system may access software. Instead, the time stamp of Komura is used for transmitting a packet without stopping event when a bit rate becomes higher. (Komura, col. 1, lines 5-12).

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons discussed above, i.e., because Komura does not teach the use of a time stamp to determine whether a second computer system can access software.

Accordingly, claims 6 and 32 provide additional grounds of patentability over the cited art.

5. Claims 7, 20, and 33 are Patentable Over the Cited Art

The Examiner rejected claims 7, 20, and 33 as obvious (35 U.S.C. §103(a)) over Davis in view of Takahashi (U.S. Patent No. 6,195,432). Applicants traverse and submit that these claims are patentable over the cited art because they depend from one of claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-40 are patentable over the art of record. Applicants submit that no additional fees are needed. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: February 13, 2006

By: _____
David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984